PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-126915
(43)Date of publication of application : 22.04.2004

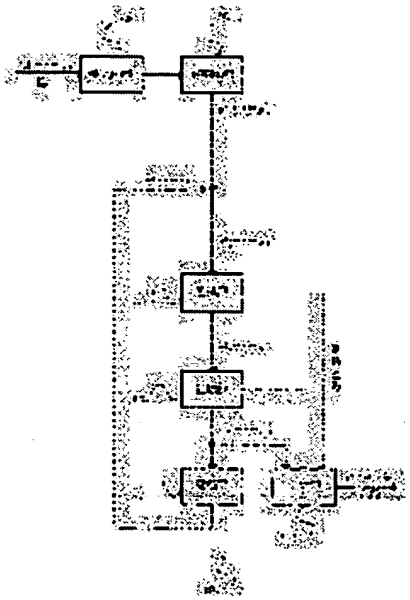
(51)Int.Cl. G06F 7/58
G09C 1/00
H03K 3/84

(21)Application number : 2002-289825
(22)Date of filing : 02.10.2002

(71)Applicant : COMMUNICATION RESEARCH LABORATORY
(72)Inventor : UMENO TAKESHI

(54) RANDOM NUMBER SEQUENCE GENERATION DEVICE, RANDOM NUMBER SEQUENCE GENERATION METHOD, AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a random number sequence generation device by which a generated random number sequence has favorable natures as the random number sequence, and to provide a random number sequence generation method, and a program for materializing the device and the method by means of a computer.
SOLUTION: The pilot reception section 102 of the random number sequence generation device 101 receives the integer string of w bits as a pilot. An initialization section 103 provides the integer string of the received pilot to a conversion section 104. The conversion section 104 applies conversion defined by nonlinear conversion g to the respective provided integer strings to obtain the integer string of the w bits. A rotation section 105 conducts the specified rotation operation by understanding the obtained integer string as the bit string of wn bits to obtain the integer string of the w bits from the obtained bit string of the wn bits. An output section 107 determines that whether or not conversion in the conversion section 104 and rotation in the rotation section 105 are repeated by the specified number of times, and finally, outputs the integer string obtained from the rotation section 105 as the random number sequence. A renewal section 106 provides the integer string obtained from the rotation section 105 to the conversion section 104 to repeat processing.



LEGAL STATUS

[Date of request for examination] 02.10.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-126915
(P2004-126915A)
(43)公開日　平成16年4月22日(2004.4.22)

(51)Int.Cl.[7]		F I			テーマコード（参考）
G06F	7/58	G06F	7/58	B	5J049
G09C	1/00	G09C	1/00	650B	5J104
H03K	3/84	H03K	3/84	Z	

審査請求 有　請求項の数 26　OL　（全 15 頁）

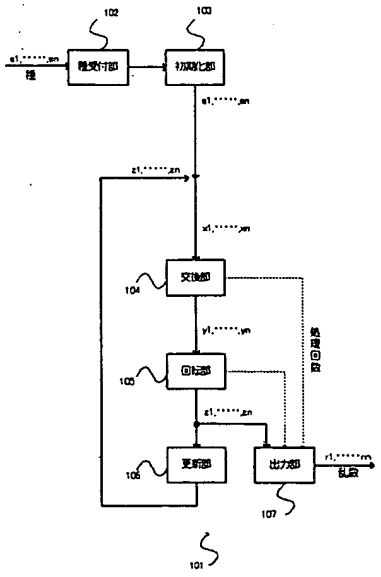
(21)出願番号　特願2002-289825(P2002-289825)
(22)出願日　平成14年10月2日(2002.10.2)

(71)出願人　301022471
独立行政法人通信総合研究所
東京都小金井市貫井北町４－２－１
(74)代理人　100095407
弁理士　木村　満
(74)代理人　100110135
弁理士　石井　裕一郎
(72)発明者　梅野　健
東京都小金井市貫井北町４－２－１　独立行政法人通信総合研究所内

Fターム(参考)　5J049 AA00 AA31 CA05
5J104 AA18 FA05 NA04 NA09 NA10 NA17

(54)【発明の名称】乱数列生成装置、乱数列生成方法、ならびに、プログラム

(57)【要約】
【課題】乱数列生成装置等を提供する。
【解決手段】乱数列生成装置１０１の種受付部１０２は、ｗビットの整数の列を種として受け付け、初期化部１０３は、当該受け付けられた種の整数列を変換部１０４に与え、変換部１０４は、当該与えられた整数列のそれぞれに対して非線型変換ｇ（・，・）により定義される変換を施してｗビットの整数の列を得て、回転部１０５は、当該得られた整数の列をｗｎビットのビット列と見て所定の回転演算を行って、得られたｗｎビットのビット列からｗビットの整数の列を得て、出力部１０７は、変換部１０４における変換ならびに回転部１０５における回転が、所定の回数繰り返されたか否かを判定し、最後に回転部１０５により得られた整数の列を、乱数列として出力し、更新部１０６は、当該回転部１０５により得られた整数の列を変換部１０４に与えて、処理を繰り返す。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ｗビットの乱数の列を生成する乱数列生成装置であって、種受付部と、初期化部と、変換部と、回転部と、更新部と、出力部と、を備え、
前記種受付部は、ｗビットの整数の列s_1，s_2，…，s_nを種として受け付け、
前記初期化部は、当該受け付けられた整数の列s_1，s_2，…，s_nを、整数列x_1，x_2，…，x_nとして前記変換部に与え、
前記変換部は、当該与えられた整数列x_1，x_2，…，x_nのそれぞれに対して所定の変換を施してｗビットの整数の列y_1，y_2，…，y_nを得て、
前記回転部は、当該整数の列y_1，y_2，…，y_nをｗｎビットのビット列と見て所定の回転演算を行って、得られたｗｎビットのビット列からｗビットの整数の列z_1，z_2，…，z_nを得て、
前記更新部は、当該整数の列z_1，z_2，…，z_nを整数列x_1，x_2，…，x_nとして前記変換部に与え、
前記出力部は、前記変換部における変換ならびに前記回転部における回転が、所定の回数繰り返された場合、最後に得られたz_1，z_2，…，z_nを、乱数列r_1，r_2，…，r_nとして出力する
ことを特徴とするもの。
【請求項２】
請求項１に記載の乱数列生成装置であって、
前記変換部は、写像ｇ（・，・）を用いて、整数ｉ　（$1 \leqq i \leqq n-1$）についての漸化式
$y_1 = g(x_n, x_1)$；
$y_{i+1} = g(x_i, x_{i+1})$
により変換を行う
ことを特徴とするもの。
【請求項３】
請求項１に記載の乱数列生成装置であって、
前記変換部は、所定の整数ｃと、写像ｇ（・，・）と、を用いて、整数ｉ　（$1 \leqq i \leqq n-1$）についての漸化式
$y_1 = g(c, x_1)$；
$y_{i+1} = g(y_i, x_{i+1})$
により変換を行う
ことを特徴とするもの。
【請求項４】
請求項１に記載の乱数列生成装置であって、
前記変換部は、写像ｇ（・，・）を用いて、整数ｉ　（$1 \leqq i \leqq n-1$）についての漸化式
$y_1 = g(c, x_1)$；
$y_{i+1} = g(x_i, x_{i+1})$
により変換を行う
ことを特徴とするもの。
【請求項５】
請求項２から４のいずれか１項に記載の乱数列生成装置であって、
当該写像ｇ（・，・）は、所定の写像ｈ（・）と所定の整数ｑ　（$0 \leqq q \leqq 2^w - 1$）により
$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$
と定義される
ことを特徴とするもの。
【請求項６】

請求項５に記載の乱数列生成装置であって、当該写像ｈ（・）は、
ｈ（ａ）　＝　ａ
と定義される
ことを特徴とするもの。
【請求項７】
請求項５に記載の乱数列生成装置であって、
当該写像ｈ（・）は、与えられた値の数値表現の所定のビットをクリアする演算により定義される
ことを特徴とするもの。
【請求項８】
請求項５に記載の乱数列生成装置であって、
当該写像ｈ（・）は、与えられた値の数値表現の所定のビットを反転する演算により定義される
ことを特徴とするもの。
【請求項９】
請求項５に記載の乱数列生成装置であって、
当該写像ｈ（・）は、与えられた値の数値表現の最下位２ビットを０１に置換する演算により定義される
ことを特徴とするもの。
【請求項１０】
請求項１から９のいずれか１項に記載の乱数列生成装置であって、
前記回転部は、当該所定の回転演算として、当該ｗｎビットのビット列を所定のビット数だけ巡回シフトする
ことを特徴とするもの。
【請求項１１】
請求項１から９のいずれか１項に記載の乱数列生成装置であって、
前記回転部は、他の乱数をさらに取得し、当該所定の回転演算は、当該整数列y_1，y_2，…，y_nを回転させる回転方向および回転ビット数は、当該他の乱数の値によって決まる
ことを特徴とするもの。
【請求項１２】
請求項１から９のいずれか１項に記載の乱数列生成装置であって、
前記回転部は、他の乱数をさらに取得し、当該所定の回転演算は、当該他の乱数が所定の値である場合、当該整数列y_1，y_2，…，y_nを所定のビット数だけある方向に回転し、そうでない場合、これとは逆の方向に回転する
ことを特徴とするもの。
【請求項１３】
ｗビットの乱数の列を生成する乱数列生成方法であって、種受付工程と、初期化工程と、変換工程と、回転工程と、更新工程と、出力工程と、を備え、
前記種受付工程では、ｗビットの整数の列s_1，s_2，…，s_nを種として受け付け、前記初期化工程では、当該受け付けられた整数の列s_1，s_2，…，s_nを、整数列x_1，x_2，…，x_nとして前記変換工程に与え、
前記変換工程では、当該与えられた整数列x_1，x_2，…，x_nのそれぞれに対して所定の変換を施してｗビットの整数の列y_1，y_2，…，y_nを得て、
前記回転工程では、当該整数の列y_1，y_2，…，y_nをｗｎビットのビット列と見て所定の回転演算を行って、得られたｗｎビットのビット列からｗビットの整数の列z_1，z_2，…，z_nを得て、
前記更新工程では、当該整数の列z_1，z_2，…，z_nを整数列x_1，x_2，…，x_nとして前記変換工程に与え、
前記出力工程では、前記変換工程における変換ならびに前記回転工程における回転が、所

定の回数繰り返された場合、最後に得られた整数の列z_1，z_2，…，z_nを、乱数列r_1，r_2，…，r_nとして出力する
ことを特徴とする方法。
【請求項１４】
請求項１３に記載の乱数列生成方法であって、
前記変換工程では、写像ｇ（・，・）を用いて、整数ｉ　（$1 \leqq i \leqq n-1$）についての漸化式
$y_1 = g(x_n, x_1)$；
$y_{i+1} = g(x_i, x_{i+1})$
により変換を行う
ことを特徴とする方法。
【請求項１５】
請求項１３に記載の乱数列生成方法であって、
前記変換工程では、所定の整数ｃと、写像ｇ（・，・）と、を用いて、整数ｉ　（$1 \leqq i \leqq n-1$）についての漸化式
$y_1 = g(c, x_1)$；
$y_{i+1} = g(y_i, x_{i+1})$
により変換を行う
ことを特徴とする方法。
【請求項１６】
請求項１３に記載の乱数列生成方法であって、
前記変換工程では、写像ｇ（・，・）を用いて、整数ｉ　（$1 \leqq i \leqq n-1$）についての漸化式
$y_1 = g(c, x_1)$；
$y_{i+1} = g(x_i, x_{i+1})$
により変換を行う
ことを特徴とする方法。
【請求項１７】
請求項１４から１６のいずれか１項に記載の乱数列生成方法であって、
当該写像ｇ（・，・）は、所定の写像ｈ（・）と所定の整数ｑ　（$0 \leqq q \leqq 2^w - 1$）により
$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$
と定義される
ことを特徴とする方法。
【請求項１８】
請求項１７に記載の乱数列生成方法であって、当該写像ｈ（・）は、
$h(a) = a$
と定義される
ことを特徴とする方法。
【請求項１９】
請求項１７に記載の乱数列生成方法であって、
当該写像ｈ（・）は、与えられた値の数値表現の所定のビットをクリアする演算により定義される
ことを特徴とする方法。
【請求項２０】
請求項１７に記載の乱数列生成方法であって、
当該写像ｈ（・）は、与えられた値の数値表現の所定のビットを反転する演算により定義される
ことを特徴とする方法。
【請求項２１】

請求項１７に記載の乱数列生成方法であって、
当該写像ｈ（・）は、与えられた値の数値表現の最下位２ビットを０１に置換する演算により定義される
ことを特徴とする方法。
【請求項２２】
請求項１３から２１のいずれか１項に記載の乱数列生成方法であって、
前記回転工程では、当該所定の回転演算として、当該ｗｎビットのビット列を所定のビット数だけ巡回シフトする
ことを特徴とする方法。
【請求項２３】
請求項１３から２１のいずれか１項に記載の乱数列生成方法であって、
前記回転工程では、他の乱数をさらに取得し、当該所定の回転演算は、当該整数列y_1，y_2，…，y_nを回転させる回転方向および回転ビット数は、当該他の乱数の値によって決まる
ことを特徴とする方法。
【請求項２４】
請求項１３から２１のいずれか１項に記載の乱数列生成方法であって、
前記回転工程では、他の乱数をさらに取得し、当該所定の回転演算は、当該他の乱数が所定の値である場合、当該整数列y_1，y_2，…，y_nを所定のビット数だけある方向に回転し、そうでない場合、これとは逆の方向に回転する
ことを特徴とする方法。
【請求項２５】
コンピュータを、請求項１から１２のいずれか１項に記載の乱数列生成装置として機能させることを特徴とするプログラム。
【請求項２６】
コンピュータに、請求項１３から２４のいずれか１項に記載の乱数列生成方法を実行させることを特徴とするプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、乱数列生成装置、乱数列生成方法、ならびに、プログラムに関する。
【０００２】
【従来の技術】
従来から、種々の乱数列生成のための技術が提案されている。これらの技術によって得られた乱数は、たとえば、モンテカルロ法による各種の物理現象、化学現象などの模擬実験や、秘密通信のブロック暗号システムにおいて用いられる。
【０００３】
【発明が解決しようとする課題】
さて、このような乱数列の生成技術においては、得られた乱数列に含まれる数値の分布ができるだけ一様であることや、当該数値のコンピュータにおける数値表現の所定のビットのみを見た場合に、当該ビットの「０」と「１」の出現頻度にできるだけ偏りがないことや、乱数列の周期ができるだけ長いことなど、種々の性質を満たすことが望ましい。
【０００４】
本発明は、生成される乱数列が乱数列として好ましい性質を有するような乱数列生成装置、乱数列生成方法、ならびに、これらをコンピュータによって実現するためのプログラムを提供することを目的とする。
【０００５】
【課題を解決するための手段】
以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。
【０００６】

本発明の第１の観点に係る乱数生成装置は、ｗビットの乱数の列を生成し、種受付部と、初期化部と、変換部と、回転部と、更新部と、出力部と、を備え、以下のように構成する。

【０００７】

すなわち、種受付部は、ｗビットの整数の列s_1，s_2，…，s_nを種として受け付ける。

【０００８】

一方、初期化部は、当該受け付けられた整数の列s_1，s_2，…，s_nを、整数列x_1，x_2，…，x_nとして変換部に与える。

【０００９】

さらに、変換部は、当該与えられた整数列x_1，x_2，…，x_nのそれぞれに対して所定の変換を施してｗビットの整数の列y_1，y_2，…，y_nを得る。

【００１０】

そして、回転部は、当該整数の列y_1，y_2，…，y_nをｗｎビットのビット列と見て所定の回転演算を行って、得られたｗｎビットのビット列からｗビットの整数の列z_1，z_2，…，z_nを得る。

【００１１】

一方、更新部は、当該整数の列z_1，z_2，…，z_nを整数列x_1，x_2，…，x_nとして変換部に与える。

【００１２】

さらに、出力部は、変換部における変換ならびに回転部における回転が、所定の回数繰り返された場合、最後に得られた整数の列z_1，z_2，…，z_nを、乱数列r_1，r_2，…，r_nとして出力する。

【００１３】

また、本発明の乱数列生成装置において、変換部は、写像ｇ（・，・）を用いて、整数ｉ（１≦ｉ≦ｎ－１）についての漸化式

$y_1 = g(x_n, x_1)$；

$y_{i+1} = g(x_i, x_{i+1})$

により変換を行うように構成することができる。

【００１４】

また、本発明の乱数列生成装置において、変換部は、所定の整数ｃと、写像ｇ（・，・）と、を用いて、整数ｉ（１≦ｉ≦ｎ－１）についての漸化式

$y_1 = g(c, x_1)$；

$y_{i+1} = g(y_i, x_{i+1})$

により変換を行うように構成することができる。

【００１５】

また、本発明の乱数列生成装置において、変換部は、写像ｇ（・，・）を用いて、整数ｉ（１≦ｉ≦ｎ－１）についての漸化式

$y_1 = g(c, x_1)$；

$y_{i+1} = g(x_i, x_{i+1})$

により変換を行うように構成することができる。

【００１６】

また、本発明の乱数列生成装置において、当該写像ｇ（・，・）は、所定の写像ｈ（・）と所定の整数ｑ　（$0 \leqq q \leqq 2^w - 1$）により

$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$

と定義されるように構成することができる。

【００１７】

また、本発明の乱数列生成装置において、当該写像ｈ（・）は、

$h(a) = a$

と定義されるように構成することができる。

【００１８】
また、本発明の乱数列生成装置において、当該写像ｈ（・）は、与えられた値の数値表現の所定のビットをクリアする演算により定義されるように構成することができる。
【００１９】
また、本発明の乱数列生成装置において、当該写像ｈ（・）は、与えられた値の数値表現の所定のビットを反転する演算により定義されるように構成することができる。
【００２０】
また、本発明の乱数列生成装置において、当該写像ｈ（・）は、与えられた値の数値表現の最下位２ビットを０１に置換する演算により定義されるように構成することができる。
【００２１】
また、本発明の乱数列生成装置において、回転部は、当該所定の回転演算として、当該ｗｎビットのビット列を所定のビット数だけ巡回シフトするように構成することができる。
【００２２】
また、本発明の乱数列生成装置において、回転部は、他の乱数をさらに取得し、当該所定の回転演算は、当該整数列y_1，y_2，…，y_nを回転させる回転方向および回転ビット数は、当該他の乱数の値によって決まるように構成することができる。
【００２３】
また、本発明の乱数列生成装置において、回転部は、他の乱数をさらに取得し、当該所定の回転演算は、当該他の乱数が所定の値である場合、当該整数列y_1，y_2，…，y_nを所定のビット数だけある方向に回転し、そうでない場合、これとは逆の方向に回転するように構成することができる。
【００２４】
本発明の他の観点に係る乱数列生成方法は、ｗビットの乱数の列を生成し、種受付工程と、初期化工程と、変換工程と、回転工程と、更新工程と、出力工程と、を備え、以下のように構成する。
【００２５】
すなわち、種受付工程では、ｗビットの整数の列s_1，s_2，…，s_nを種として受け付ける。
【００２６】
一方、初期化工程では、当該受け付けられた整数の列s_1，s_2，…，s_nを、整数列x_1，x_2，…，x_nとして変換工程に与える。
【００２７】
さらに、変換工程では、当該与えられた整数列x_1，x_2，…，x_nのそれぞれに対して所定の変換を施してｗビットの整数の列y_1，y_2，…，y_nを得る。
【００２８】
そして、回転工程では、当該整数の列y_1，y_2，…，y_nをｗｎビットのビット列と見て所定の回転演算を行って、得られたｗｎビットのビット列からｗビットの整数の列z_1，z_2，…，z_nを得る。
【００２９】
一方、更新工程では、当該整数の列z_1，z_2，…，z_nを整数列x_1，x_2，…，x_nとして変換工程に与える。
【００３０】
さらに、出力工程では、変換工程における変換ならびに回転工程における回転が、所定の回数繰り返された場合、最後に得られた整数の列z_1，z_2，…，z_nを、乱数列r_1，r_2，…，r_nとして出力する。
【００３１】
また、本発明の乱数列生成方法において、変換工程では、写像ｇ（・，・）を用いて、整数ｉ　（$1 \leqq i \leqq n-1$）についての漸化式
$y_1 = g(x_n, x_1)$；
$y_{i+1} = g(x_i, x_{i+1})$

により変換を行うように構成することができる。

【００３２】

また、本発明の乱数列生成方法において、変換工程では、所定の整数ｃと、写像ｇ（・，・）と、を用いて、整数ｉ　（１≦ｉ≦ｎ－１）についての漸化式

$y_1 = g(c, x_1)$；

$y_{i+1} = g(y_i, x_{i+1})$

により変換を行うように構成することができる。

【００３３】

また、本発明の乱数列生成方法において、変換工程では、写像ｇ（・，・）を用いて、整数ｉ　（１≦ｉ≦ｎ－１）についての漸化式

$y_1 = g(c, x_1)$；

$y_{i+1} = g(x_i, x_{i+1})$

により変換を行うように構成することができる。

【００３４】

また、本発明の乱数列生成方法において、当該写像ｇ（・，・）は、所定の写像ｈ（・）と所定の整数ｑ　（０≦ｑ≦2^w－１）により

$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$

と定義されるように構成することができる。

【００３５】

また、本発明の乱数列生成方法において、当該写像ｈ（・）は、

$h(a) = a$

と定義されるように構成することができる。

【００３６】

また、本発明の乱数列生成方法であって、当該写像ｈ（・）は、与えられた値の数値表現の所定のビットをクリアする演算により定義されるように構成することができる。

【００３７】

また、本発明の乱数列生成方法において、当該写像ｈ（・）は、与えられた値の数値表現の所定のビットを反転する演算により定義されるように構成することができる。

【００３８】

また、本発明の乱数列生成方法において、当該写像ｈ（・）は、与えられた値の数値表現の最下位２ビットを０１に置換する演算により定義されるように構成することができる。

【００３９】

また、本発明の乱数列生成方法において、回転工程では、当該所定の回転演算として、当該ｗｎビットのビット列を所定のビット数だけ巡回シフトするように構成することができる。

【００４０】

また、本発明の乱数列生成方法において、回転工程では、他の乱数をさらに取得し、当該所定の回転演算は、当該整数列$y_1, y_2, \cdots, y_n$を回転させる回転方向および回転ビット数は、当該他の乱数の値によって決まるように構成することができる。

【００４１】

また、本発明の乱数列生成方法において、回転工程では、他の乱数をさらに取得し、当該所定の回転演算は、当該他の乱数が所定の値である場合、当該整数列$y_1, y_2, \cdots, y_n$を所定のビット数だけある方向に回転し、そうでない場合、これとは逆の方向に回転するように構成することができる。

【００４２】

本発明の他の観点に係るプログラムは、コンピュータを、上記の乱数列生成装置として機能させるように構成する。

【００４３】

本発明の他の観点に係るプログラムは、コンピュータに、上記の乱数列生成方法を実行させるように構成する。

【００４４】
これらのプログラムは、コンパクトディスク、フレキシブルディスク、ハードディスク、光磁気ディスク、ディジタルビデオディスク、磁気テープ、半導体メモリ等のコンピュータ読取可能な情報記録媒体に記録することができる。
【００４５】
上記プログラムは、当該プログラムが実行されるコンピュータとは独立して、コンピュータ通信網を介して配布・販売することができる。また、上記情報記録媒体は、当該コンピュータとは独立して配布・販売することができる。
【００４６】
【発明の実施の形態】
以下に本発明の実施形態を説明する。なお、以下に説明する実施形態は説明のためのものであり、本願発明の範囲を制限するものではない。したがって、当業者であればこれらの各要素もしくは全要素をこれと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も本願発明の範囲に含まれる。
【００４７】
（発明の実施の形態）
以下で説明する本発明の実施形態においては、「ｗビットの数値表現による乱数」の列を生成するために、有限体上の非線型変換として、所定の写像ｈ（・）と所定の整数ｑ　（０≦ｑ≦$2^{w}-1$）とを用いて
$g(a,b) = 2b^{2} + h(a)b + q \pmod{2^{w}}$
により定義される写像ｇ（・，・）を用いる。
【００４８】
写像ｈ（・）としては、恒等写像
ｈ（ａ）　＝　ａ
を用いることができる。
【００４９】
また、所定のマスク値ＭＡＳＫを利用することにより、与えられた値ａの数値表現の所定のビットをクリアする演算
ｈ（ａ）　＝　ａ　ａｎｄ　ＭＡＳＫ
や、所定のビットを反転する演算
ｈ（ａ）　＝　ａ　ｘｏｒ　ＭＡＳＫ
を採用してもよい。
【００５０】
さらに、最下位の２ビットを値０１に変換する演算
ｈ（ａ）　＝　（ａ　ａｎｄ　（ｎｏｔ　３））　ｏｒ　１
などを採用することができる。
【００５１】
ここで、各演算子は値ａの数値表現（整数表現）に対するもので、ａｎｄはビット積（ビットアンド）、ｘｏｒはビット排他的和（ビットエクスクルーシブオア）、ｎｏｔはビット反転（ビットノット）、ｏｒはビット和（ビットオア）にそれぞれ相当するものである。
【００５２】
したがって、これらの演算は、コンピュータにおいては桁上がりや桁下がりなどをとりたてて考慮せずに、ｗビットの整数演算として用意されているものをそのまま適用して実現することができる。
【００５３】
またｗの値は、当該コンピュータのＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）に用意されている機械語のビット幅、もしくは、これよりも小さい幅に対応させることが望ましい。
【００５４】

現在のところ、世界最高速のブロック暗号技術といわれているＲＣ６は、有限体上の非線型変換

$f(x) = 2x^2 + x \pmod{2^w}$

を用いることによって実現されており、これによって、ある種から生成される乱数列は、これとは異なる種から生成される乱数列とは常に異なるものであり（１対１性）、生成される乱数列の最長周期が2^{w-1}となっている。

【００５５】

本実施形態において採用される写像ｇ（・，・）は、ＲＣ６における有限体上の非線型変換をさらに一般化したものであり、

$h(a) = 1$；

$q = 0$

としたｇ（・，・）を採用した場合には、ＲＣ６と同等の乱数列の生成能力を有する。なお、本発明においては、上記のＲＣ６同等の写像の以外の写像を選択できるため、さまざまなバリエーションの乱数を得ることができる。

【００５６】

また、これ以外の演算や値を選択した場合にも、良好な乱数列が得られることが、実験により実証されている。

【００５７】

図１は、本実施形態に係る乱数生成装置の概要構成を示す模式図である。図２は、本実施形態に係る乱数生成装置において実行させる処理の制御の流れを示すフローチャートである。以下、これらの図を参照して、本実施形態について、詳細に説明する。

【００５８】

乱数列生成装置１０１は、ｗビットの乱数の列を生成し、種受付部１０２と、初期化部１０３と、変換部１０４と、回転部１０５と、更新部１０６と、出力部１０７と、を備える。

【００５９】

まず、乱数列生成装置１０１の種受付部１０２は、ｗビットの整数の列$s_1, s_2, \cdots, s_n$を種として受け付ける（ステップＳ２０１）。

【００６０】

典型的には、$s_1, s_2, \cdots, s_n$は、乱数列生成装置が有するＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）等のメモリに格納されるが、ＣＰＵが有するキャッシュに格納してもよいし、ハードディスク等の読み書き可能な外部記録媒体に一時的に記憶してもよい。

【００６１】

ついで、初期化部１０３は、当該受け付けられた$s_1, s_2, \cdots, s_n$を、整数列$x_1, x_2, \cdots, x_n$として変換部１０４に与える（ステップＳ２０２）。

【００６２】

ここで、$x_1, x_2, \cdots, x_n$も同様に、ＲＡＭ等のメモリに格納される。この場合、初期化部１０３が実行する処理は、$s_1, s_2, \cdots, s_n$に対応するメモリから$x_1, x_2, \cdots, x_n$に対応するメモリへの値の転送によって実現することができる。

【００６３】

さらに、変換部１０４は、当該与えられた整数列$x_1, x_2, \cdots, x_n$のそれぞれに対して上記の非線型変換ｇ（・，・）により定義される変換を施してｗビットの整数の列$y_1, y_2, \cdots, y_n$を得る（ステップＳ２０３）。

【００６４】

当該変換としては以下のような漸化式により定義されるものを採用することができる。

【００６５】

（１）整数ｉ　（$1 \leqq i \leqq n-1$）についての漸化式

$y_1 = g(x_n, x_1)$；

$y_{i+1} = g(x_i, x_{i+1})$

により変換を行う。

【００６６】

（２）所定の整数ｃを用いて、整数ｉ　（１≦ｉ≦ｎ－１）についての漸化式

$y_1 = g(c, x_1)$；

$y_{i+1} = g(y_i, x_{i+1})$

により変換を行う。

【００６７】

（３）整数ｉ　（１≦ｉ≦ｎ－１）についての漸化式

$y_1 = g(c, x_1)$；

$y_{i+1} = g(x_i, x_{i+1})$

により変換を行う。

【００６８】

これらの計算は、ＣＰＵが有するＡＬＵ（Ａｒｉｔｈｍｅｔｉｃ　Ｌｏｇｉｃ　Ｕｎｉｔ）を用いて実現することができる。y_1，y_2，…，y_nもまた、メモリ等に格納される。

【００６９】

そして、回転部１０５は、当該y_1，y_2，…，y_nをｗｎビットのビット列と見て所定の回転演算を行って、得られたｗｎビットのビット列からｗビットの整数の列z_1，z_2，…，z_nを得る（ステップＳ２０４）。

【００７０】

所定の回転演算としては、以下のようなものを採用することができる。

【００７１】

（１）ｗｎビットのビット列を所定のビット数だけ巡回シフトするもの。図３に、この巡回シフトとして、ｗ＝４，ｎ＝４であって、y_1，y_2，…，y_4をビッグエンディアンに配列して、１ビット左にシフトする場合の概要構成を示した。

【００７２】

（２）他の乱数をさらに取得して、これによって、回転方向および回転ビット数を決めるもの。たとえば、以下のような態様が考えられる。

（ｉ）得られた乱数が所定の値である場合ある方向に所定のビット数だけ回転し、そうでない場合、これとは逆の方向に所定のビット数だけ回転させる。たとえば、得られた乱数が奇数の場合は左に１ビット、偶数の場合は右に１ビット巡回シフトする。

（ｉｉ）得られた乱数の値のビット数だけ左に巡回シフトする。

（ｉｉｉ）得られた乱数の値を符号付整数と見て、その符号付整数の値だけ左に巡回シフトする（負の場合は、その絶対値分だけ右に巡回シフトすることになる）。

【００７３】

これは、メモリ等に格納されたy_1，y_2，…，y_nを、ＣＰＵにとって自然なビット幅単位で、桁上がり・桁下がりを考慮しつつ、順次巡回シフトすることによって実現することができる。この場合、得られるz_1，z_2，…，z_nは、y_1，y_2，…，y_nが格納されていたメモリ内の領域に新たな値として格納されることとなる。

【００７４】

さらに、出力部１０７は、変換部１０４における変換ならびに回転部１０５における回転が、所定の回数繰り返されたか否かを判定する（ステップＳ２０６）。

【００７５】

たとえば、ステップＳ２０１の前において、メモリ内に用意されたカウンタ変数に「所定の回数の値」を代入し、ステップＳ２０５とステップＳ２０６の間において当該カウンタ変数の値を１減じ、ステップＳ２０６においては、当該カウンタ変数の値が０になったか否かを判定することによって、実現することができる。

【００７６】

所定の回数繰り返された場合（ステップＳ２０６；Ｙｅｓ）最後に得られたz_1，z_2，…，z_nを、乱数列r_1，r_2，…，r_nとして出力して（ステップＳ２０７）、乱数列

の生成を終了する。

【００７７】

一方、所定の回数繰り返されていない場合（ステップＳ２０６；Ｎｏ）、更新部１０６は、当該z_1，z_2，…，z_nを整数列x_1，x_2，…，x_nとして変換部１０４に与えて（ステップＳ２０５）、ステップＳ２０３に戻り、変換（ステップＳ２０３）、回転（ステップＳ２０４）の処理を繰り返す。

【００７８】

これは、z_1，z_2，…，z_nが格納されているメモリ等内の値を、x_1，x_2，…，x_nが格納されているメモリ等へ転送することによって実現できる。

【００７９】

乱数列生成装置１０１においては、図示しない記憶部が存在し、その記憶部は、s_1，s_2，…，s_n、x_1，x_2，…，x_n、y_1，y_2，…，y_n、z_1，z_2，…，z_n、r_1，r_2，…，r_nなどを異なる領域に、もしくは、値の利用の依存関係を分析することにより、同じ領域に記憶する（たとえば、y_1，y_2，…，y_nとz_1，z_2，…，z_n等。）ような構成をとることができる。また、各部は、上記の共有メモリを用いて互いに計算した値をやりとりするのである。

【００８０】

図４は、本実施形態の乱数列生成装置１０１が実現されるコンピュータの典型的な概要構成を示す模式図である。以下、本図を参照して説明する。

【００８１】

コンピュータ３０１は、ＣＰＵ　３０２によって制御される。コンピュータ３０１に電源が投入されると、ＣＰＵ　３０２は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）３０３に用意されたＩＰＬ（Ｉｎｉｔｉａｌ　Ｐｒｏｇｒａｍ　Ｌｏａｄｅｒ）を実行する。

【００８２】

そして、ＩＰＬの実行により、フレキシブルディスクドライブ３０４に装着されたフレキシブルディスクやハードディスク３０５等に記録されたＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）がロードされ、ユーザからの各種の指示入力を受け付けることができるようになる。

【００８３】

ユーザは、キーボード３０６やマウス３０７を操作して、コンピュータ３０１に対して各種の指示入力を与える。

【００８４】

これに応じて、ＯＳは、ハードディスク３０５やＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　ＤｉｓｋＲＯＭ）ドライブ３０８に装着されたＣＤ－ＲＯＭに記録されたプログラムや各種のデータをＣＰＵ　３０２に実行させ、実行の過程やその結果をディスプレイ３０９に表示する。

【００８５】

また、ＣＰＵ　３０２は、一時的な記憶域として、ＲＡＭ　３１１を利用する。ＲＡＭ　３１１は、上記のように、計算の途中で利用される各種の数列を記憶するために用いられる。

【００８６】

さらに、ＣＰＵ　３０２は、プログラムの実行の過程において、ハードディスク３０５に、生成された乱数列などの処理の結果や途中経過などの情報を保存することができる。

【００８７】

なお、本実施形態における演算は、上記のように、きわめて単純なビット演算に還元することができる。したがって、専用の電子回路（加算器、減算器、シフタ、ラッチ等）を組み合わせて乱数列生成装置１０１を構成することができるほか、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）やＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）などのような電子回路の構成状態を可変に変更できる電子素子を利用して、乱数列生成装置１０１を構成することができ、これらの態様も本発明の

範囲に含まれる。

【００８８】

（実験の結果）

上記実施形態に係る乱数列生成装置１０１を用いて、以下の諸元で乱数列を生成させた。

Ｗ　＝　３２，

ｎ　＝　３２，

$g(a, b) = 2b^2 + h(a)b$

【００８９】

ただし、写像ｈ（・）は、与えられた値の数値表現の最下位２ビットを０１に置換する演算により定義される。

【００９０】

また、変換および回転は、それぞれ１ラウンドごとに１回とした。すなわち、「所定の回数の繰り返し」は１回である。

【００９１】

出力されるのは、全部でｗｎ　＝　１０２４ビットの乱数列$r_1, r_2, \cdots, r_{1024}$である。

【００９２】

これに対して２００００×８９９９９種類の種を与え、２００００×８９９９９ラウンドだけ乱数列$r_1, r_2, \cdots, r_{1024}$を出力させた。

【００９３】

そして、これに対して乱数列のランダム性を検査する標準的なテストであるＦＩＰＳ　１４０－１ならびにＦＩＰＳ　１４０－２のうち、標準セキュリティ規格にあるランダム性検査テストを、１０２４ビットの乱数列の中の各ビット位置毎に適用して、本実施形態の乱数列の性質を検査した。

【００９４】

これらのテストにおいては、各ビット位置から２００００ビットのビット列を取り出し、その２００００ビットのビット列に対して、以下が行われる。

モノビットテスト（ｍｏｎｏｂｉｔ　ｔｅｓｔ）。所定の位置のビットの値の出現頻度に偏りがないか否かを調べるもの。

ポーカーテスト（ｐｏｋｅｒ　ｔｅｓｔ）。２００００ビットを５０００個の４ビットパターンに分割し、その４ビットパターンの出現頻度に偏りがないか否かを調べるもの。

ランズテスト（ｒｕｎｓ　ｔｅｓｔ）。乱数列から所定の長さの連を切り出した場合に、当該長さの連の出現頻度に偏りがないか否かを調べるもの。長さとしては１～６を用いる。

ロングランズテスト（ｌｏｎｇ　ｒｕｎｓ　ｔｅｓｅｔ）。ランズテストと同様であるが、ＦＩＰＳ　１４０－１の場合は３４以上の連が存在する場合ランダム性が否定され、ＦＩＰＳ　１４０－１の場合は２６以上の連が存在する場合ランダム性が否定される。

【００９５】

実験の結果、ＦＩＰＳ　１４０－１においては、生成された１０２４ビット×８９９９９サンプルの２００００ビット列は、すべて、定められた基準をクリアした。

【００９６】

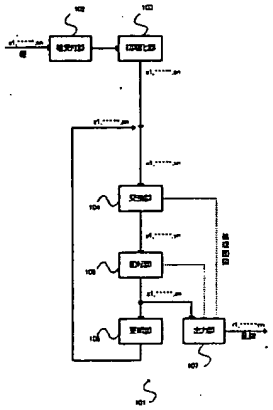
また、ＦＩＰＳ　１４０－２においては、生成された１０２４ビット×８９９９９サンプルの２００００ビット列の内、９９．９２パーセントのサンプルが、定められた基準をクリアした。

【００９７】

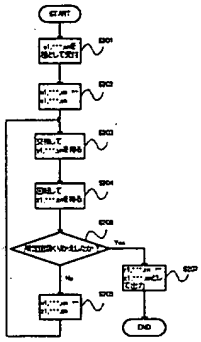
また、本技術をＸＩＬＩＮＸ（登録商標）社のＶｅｒｔｅｘ　ｘｃｖ１０００（システムゲート数は１００万）のＦＰＧＡに実装したところ、本アルゴリズムの並列性から、２５．６２Ｇビット／ｓｅｃのスピードで乱数列を生成させることができた。すなわち、本技術をＦＰＧＡ等のハードウェアに実装すると、高速性の上で多大なメリットを得ることができる。

【００９８】
このようにして、本実施形態によって生成された乱数列は極めて性質が良いものであり、秘密通信の暗号化の分野や物理現象、化学現象などの模擬実験の分野で有用であり、ハードウェア上で高速に良好なランダム性を持つ乱数列を出力するのに極めて有用であることが示された。
【００９９】
【発明の効果】
以上説明したように、本発明によれば、生成される乱数列が乱数列として好ましい性質を有するような乱数列生成装置、乱数列生成方法、ならびに、これらをコンピュータによって実現するためのプログラムを提供することができる。
【図面の簡単な説明】
【図１】本発明の実施形態に係る乱数列生成装置の概要構成を示す模式図である。
【図２】本実施形態の乱数列生成装置において実行される乱数列生成処理の制御の流れを示すフローチャートである。
【図３】本実施形態の乱数列生成装置の回転部において実行される回転演算の様子を示す説明図である。
【図４】本実施形態の乱数列生成装置が実現される典型的なコンピュータの概要構成を示す模式図である。
【符号の説明】
１０１　乱数列生成装置
１０２　種受付部
１０３　初期化部
１０４　変換部
１０５　回転部
１０６　更新部
１０７　出力部
３０１　コンピュータ
３０２　ＣＰＵ
３０３　ＲＯＭ
３０４　フレキシブルディスクドライブ
３０５　ハードディスク
３０６　キーボード
３０７　マウス
３０８　ＣＤ－ＲＯＭドライブ
３０９　ディスプレイ
３１１　ＲＡＭ

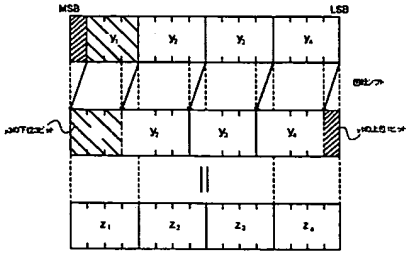
【図１】



【図２】



【図３】



【図４】